REMARKS

This paper is submitted in reply to the Office Action dated March 21, 2007. A request for a one month extension of time accompanies this paper, and therefore, the period for response extends up to and includes July 23, 2007 (as July 21, 2007 is a Saturday). Reconsideration and allowance of all pending claims are respectfully requested.

In the subject Office Action, claims 1-11, 13-14, 17-27 and 29-34 were rejected under 35 U.S.C. § 101. Moreover, claims 1-4, 6-20 and 22-34 were rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 6,950,937 to Jakobsson et al. Claims 5 and 21 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Jakobsson et al. in view of WO 02/48857 A2 to Elbe et al.

Applicant respectfully traverses the Examiner's rejections to the extent that they are maintained. Applicant has canceled claims 5, 9-12, 21, 25-28 and 34 and amended claims 1, 17 and 33. Applicant respectfully submits that no new matter is being added by the above amendments, as the amendments are fully supported in the specification, drawings and claims as originally filed. Applicant also notes that the amendments made herein are being made only for facilitating expeditious prosecution of the aforementioned claimed subject matter. Applicant is not conceding in this application that the originally-claimed subject matter is not patentable over the art cited by the Examiner, and Applicant respectfully reserves the right to pursue this and other subject matter in one or more continuation and/or divisional patent applications.

Now turning to the subject Office Action and specifically with regard to the §101 rejections, while Applicant does not agree with the rejection, the Examiner will nonetheless note that Applicant has amended claims 1 and 17 to incorporate the subject matter of claims 12 and 28, respectively, which were not rejected on the basis of §101. Claims 12 and 28 have accordingly been canceled. Claim 33 has also been amended to recite the subject matter of claim 28, and as such is statutory for the same reason. In addition, claim 33 has been amended to recite a "computer readable recordable storage medium," support for which may be found on page 11 of the Application as filed. Claim 34 has also been canceled. Withdrawal of the § 101 rejections is therefore respectfully requested.

Next turning to the art-based rejections, and specifically to the Examiner's rejection of independent claim 1, this claim generally recites a method of initiating performance of a computation on at least one untrusted computer. The method comprises partitioning the computation into a plurality of computational units that are combinable to generate a result for the computation, generating at least one distractive computational unit, initiating execution of both the at least one distractive computational unit and at least one of the plurality of computational units on the untrusted computer to inhibit reconstitution of the computation by an untrusted party.

In addition, claim 1 has been amended to incorporate the subject matter of claims 5 and 11, and now additionally recites in part that:

- the distractive computational unit comprises a dummy computational unit;
- the computation includes a plurality of arguments;
- partitioning the computation into the plurality of computational units comprises partitioning using the Chinese Remainder Theorem (CRT);
- partitioning the computation into the plurality of computational units comprises selecting a plurality of relatively prime moduli and generating each computational unit by performing a modulo operation on each of the plurality of arguments using one of the plurality of relatively prime moduli;
- selecting the plurality of relatively prime moduli includes selecting each modulus from a superset of relatively prime moduli; and
- partitioning a plurality of computations into multiple computational units using different sets of moduli selected from the superset of relatively prime moduli.

Claims 5 and 9-11 have accordingly been canceled for consistency with the amendments to claim 1.

Claim 1 was rejected as being anticipated by Jakobsson; however, the Examiner admitted in connection with the rejection of claim 5 that Jakobsson did not disclose dummy computational units. Accordingly, as claim 1 incorporates the subject matter of claim 5, claim 1 is now novel over Jakobsson, and the rejection should with withdrawn.

In addition, Applicant respectfully submits that claim 1 is also non-obvious over Jakobsson and Elbe and the other prior art of record. First, with respect to the concept of a distractive unit being a dummy unit, as the Examiner noted, this concept is not disclosed by Jakobsson. Elbe, however, which is cited for allegedly disclosing dummy units, merely discloses the use of dummy units to be executed on different cryptographic coprocessors in a cryptographic processor, and for the purpose of inhibiting the ability to reconstruct power profiles for other coprocessors in the same processor. Applicant submits that this disclosure is insufficient to suggest modifying Jakobsson to incorporate dummy units for the purpose of inhibiting reconstruction of a computation resulting from execution of such units by an untrusted computer.

Second, claim 1 as amended recites partitioning a computation using the Chinese Remainder Theorem (CRT), and more specifically, partitioning a computation by performing a modulo operation on a plurality of arguments using one of a plurality of selected, relatively prime moduli. These concepts, which were recited in claims 9 and 10, are allegedly disclosed at cols. 1, 4 and 5 of Jakobsson. However, the cited passages do not address the use of either the CRT, or more generally, of modulo operations, to partition a computation.

Instead, these passages disclose computations such as DSA signature generation computations that happen to incorporate modulo operations. Put another way, the computations themselves incorporate modulo operations, but modulo operations are not used to partition a computation into multiple computational units. Claim 1, however, uses modulo operations to partition a computation into a plurality of computational units, or put another way, to determine how a computation will be partitioned into its component computational units.

In Jakobsson, computations such as DSA signature generation computations are broken up according to exponents k_i. The transformation techniques described in the reference, replication, dependency, blinding and permutation (cols. 5-8) all operate on exponents within an exponent vector G, and Applicant submits that, based upon the Examiner's interpretation of other elements of the claims, it is evident that the Examiner is

interpreting the exponent vector G as the "computation" and the exponents k_i in the vector as the "computational units" for the purpose of applying Jakobsson to the claims at issue (see, e.g., col. 7, lines 60-63, "This input is denoted herein G_1 . . . and represents [sic] computational task for the DSA digital signature protocol.") However, there is no partitioning of a computational task in Jakobsson that relies on modulo operations to determine how the task is broken up into computational units. In no type of transform operation (replication, dependency, blinding and permutation) is any modulo operation ever used to select or modify an exponent in the exponent vector. In fact, for the blinding operation, the only modifications being performed on computational units rely on applying random and secret offsets (col. 6, lines 42-45). No modulo operations are ever used to either modify an exponent or determine what exponents are provided within an exponent vector.

Claim 1 recites that each computational unit is generated in connection with partitioning the computation by performing a modulo operation on each of the plurality of arguments in the computation using one of a plurality of relatively prime moduli. Claim 1 also recites that the partitioning of a computation includes selecting a plurality of relatively prime moduli. Jakobsson, however, does not disclose performing any type of modulo operation on arguments in a computation for the purpose of partitioning the computation, nor does the reference disclose selecting relatively prime moduli. While modulo operations are disclosed in Jakobsson, it is evident from the disclosure that these modulo operations are not used to partition an operation into multiple computational units. Jakobsson therefore does not disclose or suggest this aspect of claim 1.

Furthermore, Elbe adds nothing to the rejection in this regard, as Elbe similarly fails to disclose or suggest the use of modulo operations to determine how to partition a computation into multiple computational units.

Third, claim 1 as amended also recites the concept of partitioning a plurality of computations into multiple computational units using different sets of moduli selected from a superset of relatively prime moduli, which was originally recited in claim 11. In rejecting claim 11, the Examiner relied on col. 5, lines 1-17 of Jakobsson; however, this

passage discloses only that modulo operations can be performed as part of a DSA signature generation computation. There is nothing in this passage, however, regarding selecting moduli from a superset of relatively prime moduli, doing so differently for different computations, or for selecting those moduli for the purpose of partitioning computations into computational units. As noted above, Jakobsson does not use modulo operations to partition computations, and accordingly, Applicant submits that Jakobsson cannot be interpreted to disclose or suggest selecting sets of moduli from a superset of relatively prime moduli to partition computations in the manner recited in claim 1.

Furthermore, as Elbe does not address the use of modulo operations to partition computations, Applicant submits that the combination of Elbe likewise does not suggest selecting sets of moduli from a superset of relatively prime moduli to partition computations in the manner recited in claim 1.

Accordingly, the combination of Jakobsson and Elbe does not disclose or suggest each and every feature of claim 1, and claim 1 is therefore non-obvious over the proposed combination. Applicant also submits that the Examiner has provided no objective reason why one of ordinary skill in the art would be motivated by Elbe or any other art to modify Jakobsson to use modulo operations to partition a computation, or to do so by selecting sets of moduli from a superset of relatively prime moduli. Accordingly, claim 1 is non-obvious over the Jakobsson and Elbe. Reconsideration and allowance of claim 1, and of claims 2-4, 6-8 and 13-16 that depend therefrom, are therefore respectfully requested.

Next with regard to the rejection of independent claims 17 and 33, these claims have been amended in a similar manner to claim 1, and in particular, to incorporate the subject matter of claims 21 and 27. Claims 21 and 25-27 have also been canceled for consistency with the amendments to claim 17. As discussed above in connection with claim 1, Jakobsson and Elbe do not disclose or suggest, among other features, the use of modulo operations to determine how to partition a computation into multiple computational units, or to select sets of moduli from a superset of relatively prime moduli to partition computations. Applicant therefore respectfully submits that claims 17 and 33 are patentable over Jakobsson and Elbe for the same reasons as presented above for claim

1. Reconsideration and allowance of independent claims 17 and 33, and of claims 18-20, 22-24 and 29-32 that depend therefrom, are therefore respectfully requested.

In summary, Applicant respectfully submits that all pending claims are novel and non-obvious over the prior art of record. Reconsideration and allowance of all pending claims are therefore respectfully requested. If the Examiner has any questions regarding the foregoing, or which might otherwise further this case onto allowance, the Examiner may contact the undersigned at (513) 241-2324. Moreover, if any other charges or credits are necessary to complete this communication, please apply them to Deposit Account 23-3000.

Respectfully submitted,

July 23, 2007
Date

/Scott A. Stinebruner/
Scott A. Stinebruner
Reg. No. 38,323
WOOD, HERRON & EVANS, L.L.P.
2700 Carew Tower
441 Vine Street
Cincinnati, Ohio 45202
Telephone: (513) 241-2324
Facsimile: (513) 241-6234